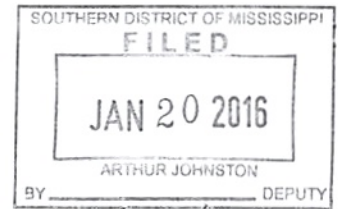


IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI  
SOUTHERN DIVISION



UNITED STATES OF AMERICA

CRIMINAL NO.

1:16cr3LG-JCG

v.

MILAD REZAEI KALANTARI

18 U.S.C. § 1349

18 U.S.C. § 371

18 U.S.C. § 1344

18 U.S.C. § 1028(a)(7)

18 U.S.C. § 1029(a)(2)

18 U.S.C. § 1029(a)(6)

18 U.S.C. § 1343

**The Grand Jury charges:**

At all times material to this Indictment,

1. “Personally identifiable information” (“PII”) means individuals’ names, social security numbers, dates of birth, addresses, phone numbers, places of work, duration of work, state driver’s license numbers, mothers’ maiden names, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.

2. “Payment card data” refers to credit, debit, and/or gift card numbers and associated data that can be used to make charges on an account. The data typically includes the payment card number, expiration date, Card Verification Value (“CVV”) number, and PII including the account holder’s name, address, and phone number.

3. “Carding” refers to an assortment of illegal activities revolving around the theft, transfer, and fraudulent use of PII and payment card data.

4. “Carders” refers to individuals who are engaged in illegal carding activity.

5. “Carding forums” are websites that provide an online marketplace for various carding activities. Typically, membership is required. Members can purchase a variety of types

of goods and services, including other individuals' PII and payment card data. The members typically communicate via email messages, private messages, or via posts to the forum.

6. "Verification" is the process by which carders confirm that payment cards are valid and usable before offering them up for sale.

7. "Digital currencies" such as Bitcoin are electronic currency systems that are not supported by any government. Digital currencies often enable individuals to transfer money anonymously to other account holders worldwide. Carders and carder forums often use digital currencies to buy and sell stolen payment card data. "Digital currency exchangers" like Liberty Reserve are businesses or individuals who allow customers to trade digital currencies for traditional currency or other digital currencies.

8. The defendant, **MILAD REZAEI KALANTARI**, is a citizen of Iran residing in Iran. He is one of the control persons and administrators for the carder forums [www.miladccshop.ru](http://www.miladccshop.ru), [www.miladccshop.com](http://www.miladccshop.com), [www.miladccstore.com](http://www.miladccstore.com), [www.miladcc.biz](http://www.miladcc.biz), [www.mcshop.biz](http://www.mcshop.biz), and [www.miladccshop.biz](http://www.miladccshop.biz) where members of the conspiracy sold stolen credit and debit card information and their associated data. He also controlled and used the email accounts [ccmilad@yahoo.com](mailto:ccmilad@yahoo.com) and [miladrk@gmail.com](mailto:miladrk@gmail.com).

#### COUNT 1

9. Paragraphs 1 through 8 of this indictment are re-alleged and incorporated by reference as if fully set forth herein.

#### *The Conspiracy*

10. Beginning on a date in or before February 2005, and continuing to the date of this Indictment, in the Southern Division of the Southern District of Mississippi and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, did knowingly and willfully conspire with others known and unknown to the Grand Jury, to violate the following sections of the United States Code:

- a. Wire fraud: that is, having devised or intended to devise a scheme and artifice to defraud and to obtain money and property by means of false and fraudulent pretenses and representations, and promises, transmits or causes to be transmitted in interstate and foreign commerce certain wire communications for the purpose of executing the scheme or artifice, in violation of Title 18, United States Code, Section 1343;
- b. Bank fraud: that is, to knowingly execute or attempt to execute a scheme and artifice to obtain funds under the custody and control of financial institutions by means of false and fraudulent pretenses and representations, in violation of Title 18, United States Code, Section 1344.

***Purpose of the Conspiracy***

11. It was the object of the conspiracy for defendant **KALANTARI** and his co-conspirators to acquire, offer for sale, sell, and transfer to others, compromised payment card data and other financial information of individuals residing in Mississippi and elsewhere, which information was to be used to engage in various types of fraudulent carding activities, including but not limited to making fraudulent charges on those accounts. The monetary proceeds were moved using numerous digital currencies.

***Manner and Means of the Conspiracy***

12. The object of the conspiracy was to be accomplished by the following manner and means:

13. It was part of the conspiracy that defendant **KALANTARI** would conspire and collaborate with other members of the conspiracy to obtain stolen credit and debit card information.

14. It was part of the conspiracy that defendant **KALANTARI** would conspire and collaborate with other members of the conspiracy to verify stolen credit and debit card information.

15. It was part of the conspiracy that defendant **KALANTARI** and his co-conspirators operated the websites: [www.miladccshop.ru](http://www.miladccshop.ru), [www.miladccshop.com](http://www.miladccshop.com), [www.miladccstore.com](http://www.miladccstore.com), [www.miladcc.biz](http://www.miladcc.biz), [www.mcshop.biz](http://www.mcshop.biz), and [www.miladccshop.biz](http://www.miladccshop.biz), which were dedicated to the sale of compromised payment card data, personal identifying information, copies of malware, and other information including usernames and passwords for victims' email accounts, shopping accounts, and romance site accounts. On these web sites, defendant **KALANTARI** and his co-conspirators offered buyers the option of choosing to buy stolen credit and debit card information from particular states within the United States, including Mississippi.

16. It was part of the conspiracy that defendant **KALANTARI** would conspire and collaborate with unknown subjects to design, create, and operate the above-mentioned websites.

17. It was part of the conspiracy that the defendant **KALANTARI**, and other members of the conspiracy, used multiple online digital currencies and exchangers to send and receive payments for the purchase, verification, and sale of compromised payment cards, personal identifying information, bank account information, and other financial information and for the administration of the web sites used in such sales.

18. It was part of the conspiracy that defendant **KALANTARI** opened and used various email accounts, including [ccmilad@yahoo.com](mailto:ccmilad@yahoo.com) and [miladrk@gmail.com](mailto:miladrk@gmail.com), to communicate with co-conspirators and customers about buying, selling, and verifying information associated with stolen payment card data and to transfer stolen credit and debit card information for these purposes.

19. It was further part of the conspiracy that defendant **KALANTARI** and his co-conspirators electronically transferred stolen payment card data, including payment card data belonging to individuals located in Mississippi, from their online carding forums to buyers, including to one or more buyers located in the Southern District of Mississippi.

***Overt Acts***

20. In order to accomplish the objects of the conspiracy, defendant **KALANTARI**, and other members of the conspiracy, committed the following overt acts, among others, in the Southern District of Mississippi and elsewhere:

***Setting Up Carding Web Sites, Email Accounts, and Digital Currency Accounts***

21. On or about February 18, 2005, defendant **KALANTARI** created an email account with Google for the account name “miladrk@gmail.com.” In the account subscriber records, MILAD identified “miladrk” as the subscriber.

22. On or about January 28, 2010, defendant **KALANTARI** registered, or caused to be registered, the domain name “miladcc.biz” with Enom Inc., a registrar located in Kirkland, Washington.

23. On or about August 2, 2010, defendant **KALANTARI** created an e-mail account with Yahoo for the account name “ccmilad@yahoo.com.” In the account subscriber records, MILAD identified “Michael Exner” as the subscriber.

24. On or about January 23, 2011, defendant **KALANTARI** created an account with Liberty Reserve. In the account subscriber records, “Milad Rezaee **KALANTARI**” is listed as the subscriber.

25. On or about May 24, 2012, defendant **KALANTARI** registered, or caused to be registered, the domain name “miladccshop.biz” with Tucows, a registrar located in Toronto, Canada.

26. On or about June 14, 2012, defendant **KALANTARI** registered, or caused to be registered, the domain name “miladccshop.ru” with Regtime, a registrar located in Samara, Russia.

27. On or about September 5, 2012, defendant **KALANTARI** registered, or caused to be registered, the domain name “miladccshop.com” with Name117 Inc., a registrar located in Denver, Colorado.

28. On or about October 4, 2012, defendant **KALANTARI** registered, or caused to be registered, the domain name “miladccstore.com” with Enom Inc., a registrar located in Kirkland, Washington.

29. On or about May 21, 2014, defendant **KALANTARI** opened a Payeer account.

30. On or about May 26, 2014, defendant **KALANTARI** opened a Payweb account.

31. On or about November 2, 2014, defendant **KALANTARI** registered, or caused to be registered, the domain name “mcshop.biz” with Regtime, a registrar located in Samara, Russia.

32. On or about May 11, 2015, defendant **KALANTARI** asked an unknown co-conspirator to look into a problem with the website [www.miladccshop.ru](http://www.miladccshop.ru).

33. Between about May 11 and May 19, 2015, defendant **KALANTARI** directed an unknown co-conspirator to re-design the administration systems for [miladccshop.ru](http://miladccshop.ru) so that defendant **KALANTARI** could add stolen credit and debit card information to the web site

without showing the name of any of the conspiracy's carder forums to anyone monitoring his online traffic.

*Storing and Offering Stolen Credit and Debit Card Information for Sale*

34. On or about December 14, 2015, defendant **KALANTARI** stored and offered for sale the stolen credit and debit card numbers and related information for at least 4,547 individuals on the www.miladccshop.ru website. These included the stolen credit and debit card numbers and related information of one or more individuals located in the Southern District of Mississippi.

*Transferring Stolen Credit and Debit Card Information*

35. The following acts in furtherance relate to the transfer of stolen credit and debit card information:

a. On or about June 5, 2014, defendant **KALANTARI** received a payment through Payeer from an unknown co-conspirator for items bought from **KALANTARI's** carder websites.

b. On or about June 7, 2014, defendant **KALANTARI** received a payment through Payeer from an unknown co-conspirator for items bought from **KALANTARI's** carder websites.

c. On or about June 10, 2014, defendant **KALANTARI** received a payment through Payeer from an unknown co-conspirator for items bought from **KALANTARI's** carder websites.

d. On or about June 12, 2014, defendant **KALANTARI** received a payment through Payeer from an unknown co-conspirator for items bought from **KALANTARI's** carder websites.

e. On or about July 30, 2014, defendant **KALANTARI** received 3,000 stolen credit and debit card numbers from a known co-conspirator.

f. On September 18, 2014, defendant **KALANTARI** received an email containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 3,060 victims, including W.S., a resident of the Southern District of Mississippi.

g. On September 18, 2014, defendant **KALANTARI** received an email from tranmailihn123@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 3,076 victims, including S.T., a resident of the Southern District of Mississippi.

h. On September 19, 2014, defendant **KALANTARI** received an email from tranmailihn123@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 220 victims, including T.U., a resident of the Southern District of Mississippi.

i. On or about September 30, 2014, defendant **KALANTARI** sent 3,000 stolen credit or debit card numbers to a known co-conspirator, for the co-conspirator to check to ensure that the cards were valid and working.

j. On October 9, 2014, defendant **KALANTARI** received an email from kakapolikpn@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 345 victims, including M.D., a resident of the Southern District of Mississippi.

k. On October 10, 2014, defendant **KALANTARI** sent an email to darkn3ssking@gmail.com containing the name, address, telephone number, credit or debit card



number, expiration date, and three-digit CVV of approximately 15,000 victims, including B.S., a resident of the Southern District of Mississippi.

l. On October 18, 2014, defendant **KALANTARI** received an email from boss\_cvv\_tk@yahoo.com.vn containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 651 victims, including Team One Communications, a business operating in the Southern District of Mississippi.

m. On or about October 21, 2014, defendant **KALANTARI** sent \$95.00 to a co-conspirator known to the grand jury.

n. On March 14, 2015, defendant **KALANTARI** received an email from qhlove@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 345 victims, including A.P., a resident of the Southern District of Mississippi, whose debit card is connected to a bank account at Keesler Federal Credit Union, a bank headquartered in the Southern District of Mississippi.

o. On April 11, 2015, defendant **KALANTARI** received an email from qhlove@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 2,159 victims, including H.W., a resident of the Southern District of Mississippi.

p. On May 19, 2015, defendant **KALANTARI** received an email from geochris\_angel@yahoo.com containing the name, address, date of birth, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 16 victims, including C.R., a resident of the Southern District of Mississippi, whose debit card was connected to a bank account with Hancock Bank, which is headquartered in Mississippi.

q. On May 25, 2015, defendant **KALANTARI** received an email from levanthien1091991@gmail.com containing the name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 994 victims, including J.P., a resident of the Southern District of Mississippi whose debit card was attached to an account with Hancock Bank, a bank headquartered in Mississippi.

36. The following acts in furtherance relate to offering to sell stolen credit and debit cards to an undercover agent in Mississippi:

a. On or about August 19, 2014, defendant **KALANTARI** and other members of the conspiracy, on their carder forum www.miladccshop.biz, advertised the sale of numerous stolen credit and debit cards to visiting members of the carding forum, including an undercover agent located in Mississippi ("UC agent").

b. In or about December 2015, defendant **KALANTARI** and other members of the conspiracy, on their carder forum www.miladccshop.ru, advertised the sale of numerous stolen credit and debit cards to visiting members of the carding forum, including an undercover agent located in Mississippi ("UC agent").

*Transferring Stolen Credit and Debit Cards to an Undercover Agent in Mississippi*

37. The following acts in furtherance relate to transferring stolen credit and debit cards to an undercover agent in Mississippi:

a. On or about December 10, 2015, the UC agent selected stolen credit and debit cards from Mississippi and purchased that stolen credit and debit card information online at www.miladccshop.ru using Bitcoins. After the UC agent purchased stolen credit and debit card information online, a screen appeared that asked the UC agent whether he wanted to open or save his purchased payment card data. When the UC agent clicked on the Save button, the stolen

credit and debit card information of approximately three Mississippi residents was downloaded to his computer in Mississippi.

b. On or about December 11, 2015, after the UC agent purchased additional stolen credit and debit card information from [www.miladccshop.ru](http://www.miladccshop.ru) using Bitcoins, a screen appeared that asked the UC agent whether he wanted to open or save his purchased payment card data. When the UC agent clicked on the Save button, the stolen credit and debit card information of approximately 45 victims was downloaded to his computer in Mississippi.

c. On or about December 14, 2015, after the UC agent purchased additional stolen credit and debit card information from [www.miladccshop.ru](http://www.miladccshop.ru) using Bitcoins, a screen appeared that asked the UC agent whether he wanted to open or save his purchased payment card data. When the UC agent clicked on the Save button, the stolen credit and debit card information of approximately 20 victims was downloaded to his computer in Mississippi.

All in violation of Sections 1349 and 2, Title 18, United States Code.

COUNT 2

38. In furtherance of the conspiracy and to carry out its objectives, the acts described in paragraphs 1 through 37 are re-alleged and incorporated as if set forth herein.

39. That from on or about February 18, 2005, and continuing until on or about the date of the indictment, in the Southern District of Mississippi, and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, and his co-conspirators, did knowing and willfully conspire with each other and with others known and unknown to the Grand Jury, to commit offenses against the United States as follows:

- a. Identity Theft as prohibited by Section 1028(a)(7), Title 18, United States Code, that is the possession, transfer, and use in or affecting interstate or foreign commerce, without lawful authority, the means of identification of another person with the intent to commit, or to aid or abet or in connection with unlawful activities that constitute violations of Federal law, or that constitute felonies under State or local law;
- b. Access Device Fraud as prohibited by Section 1029(a)(2), Title 18, United States Code, that is knowingly and with intent to defraud, traffics in one or more unauthorized access devices during a one-year period and by such conduct obtained anything of value aggregating \$1,000.00 or more during that period;
- c. Access Device Fraud as prohibited by Section 1029(a)(6)(A), Title 18, United States Code, that is knowingly and with intent to defraud, and without the authorization of the issuer of the access device, solicited a person for the purpose of offering an access device.

40. It was a part of the conspiracy that defendant **KALANTARI** and other members of the conspiracy would obtain credit and debit card information from international hackers and use that

information to obtain and traffic in unauthorized credit and debit cards as a means of identification to commit violations of federal and state law.

41. In furtherance of the conspiracy and to carry out its objectives, the acts described in paragraphs 1 through 40 are re-alleged and incorporated as if set forth herein.

All in violation of Section 371, Title 18, United States Code.

COUNTS 3 - 4

42. The allegations set forth in paragraphs 1 through 41 of the Indictment are re-alleged and incorporated as set forth herein.

43. That from on or about February 18, 2005, and continuing until on or about the date of the indictment, in the Southern District of Mississippi, and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, and his co-conspirators, devised and intended to devise, and aided and abetted others in devising, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises.

44. On or about the dates specified below, in the Southern District of Mississippi, and elsewhere, defendant **KALANTARI**, for the purpose of executing the scheme and artifice to defraud, and attempting to do so, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, the writings, signs and signals further described below on or about the dates specified:

<i>Count Number</i>	<i>Date of Wire</i>	<i>Location of Wire</i>	<i>Description of Wire</i>
3	December 10, 2015	Sent to Southern District of Mississippi	Online download of 6 compromised payment cards to UC agent in Mississippi
4	December 11, 2015	Sent to Southern District	Online download of 45

		of Mississippi	compromised payment cards to UC agent in Mississippi
--	--	----------------	--

In violation of Sections 1343 and 2, Title 18, United States Code.

#### COUNTS 5 - 7

45. The factual allegations contained in Paragraphs 1 through 44 are re-alleged and incorporated as if set forth here in their entirety.

46. On or about the dates set forth below, in the Southern District of Mississippi and elsewhere, the defendant **MILAD REZAEI KALANTARI** knowingly executed, and attempted to execute, a scheme and artifice to defraud a financial institution located in the Southern District of Mississippi, and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution, by means of materially false and fraudulent pretenses, representations, and promises:

<i>Count</i>	<i>Approximate Date</i>	<i>Victim Bank</i>	<i>Transaction</i>
5	March 14, 2015	Keesler Federal Credit Union	Co-conspirator sent defendant <b>KALANTARI</b> an email containing 345 compromised payment cards that included a Keesler Federal Credit Union customer's debit card.
6	May 19, 2015	Hancock Bank	Co-conspirator sent defendant <b>KALANTARI</b> an email titled "16 fullz – 19 May" that included a Hancock Bank customer's debit card.
7	May 25, 2015	Hancock Bank	Co-conspirator sent defendant <b>KALANTARI</b> an email containing 994 compromised payment cards that included a Hancock Bank customer's debit card.

All in violation of Sections 1344 and 2, Title 18, United States Code.

#### COUNTS 8 - 9

47. The allegations set forth in paragraphs 1 through 46 of the Indictment are re-alleged and incorporated as set forth herein.

48. On or about the dates set forth below, in the Southern District of Mississippi and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, credit and debit card and related PII of individuals residing in the Southern District of Mississippi and elsewhere, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law and that constitutes a felony under any applicable State and local law, including: access device fraud, in violation of 18 U.S.C. § 1029(a)(2) and (a)(6); wire fraud, in violation of 18 U.S.C. § 1343; and bank fraud, in violation of 18 U.S.C. § 1344.

<i>Count</i>	<i>Date</i>	<i>Action</i>	<i>Information Transferred</i>
8	December 10, 2015	UC agent in the Southern District of Mississippi downloaded purchased payment card data	Name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 6 victims, including three residents of Mississippi
9	December 11, 2015	UC agent in the Southern District of Mississippi downloaded purchased payment card data	Name, address, telephone number, credit or debit card number, expiration date, and three-digit CVV of approximately 45 victims.

In violation of Sections 1028(a)(7) and 2, Title 18, United States Code.

COUNTS 10 - 13

49. The allegations set forth in paragraphs 1 through 48 of the Indictment are re-alleged and incorporated as set forth herein.

50. On or about the dates set forth below, in the Southern District of Mississippi and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, knowingly and with intent to defraud, and in a manner affecting interstate commerce, trafficked in one or more unauthorized access devices, that is, credit and debit card information of individuals residing in the Southern District of Mississippi and elsewhere, during a one-year period and by such conduct obtained anything of value aggregating \$1,000.00 or more during that period.

<i>Count</i>	<i>Date</i>	<i>Description</i>	<i>Purchase price</i>
10	December 10, 2015	6 stolen payment cards sold to UC agent in the Southern District of Mississippi	\$63.30
11	December 11, 2015	45 stolen payment cards sold to UC agent in the Southern District of Mississippi	\$691.20
12	December 14, 2015	20 stolen payment cards sold to UC agent in the Southern District of Mississippi	\$239.00
13	December 16, 2015	22 stolen payment cards sold to UC agent in the Southern District of Mississippi	\$99.20

In violation of Sections 1029(a)(2) and 2, Title 18, United States Code.



COUNTS 14 - 16

51. The allegations set forth in paragraphs 1 through 50 of the Indictment are re-alleged and incorporated as set forth herein.

52. On or about the dates set forth below, in the Southern District of Mississippi and elsewhere, the defendant, **MILAD REZAEI KALANTARI**, knowingly and with intent to defraud, and without the authorization of the issuer of the access device, that is, credit and debit card information of individuals residing in the Southern District of Mississippi and elsewhere, solicited a person for the purpose of offering an access device.


<i>Count</i>	<i>Dates</i>	<i>Location</i>	<i>Description</i>
14	August 19, 2014	www.miladccshop.biz	Stolen credit and debit cards offered for sale
15	December 10, 2015	www.miladccshop.ru	Stolen credit and debit cards offered for sale
16	December 11, 2015	www.miladccshop.ru	Stolen credit and debit cards offered for sale

In violation of Sections 1029(a)(6) and 2, Title 18, United States Code.

**NOTICE OF INTENT TO SEEK CRIMINAL FORFEITURE**

As a result of committing the offenses alleged in this Indictment, the defendants shall forfeit to the United States all property involved in or traceable to property involved in the offenses, including but not limited to all proceeds obtained directly or indirectly from the offenses, and all property used to facilitate the offenses. Further, if any property described above, as a result of any act or omission of the defendants: (a) cannot be located upon the exercise of due diligence; (b) has been transferred or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property, which cannot be divided without difficulty, then it is the intent of the United States to seek a judgment of forfeiture of any other property of the defendants, up to the value of the property described in this notice or any bill of particulars supporting it.


All pursuant to Section 981(a)(1)(C), Title 18, United States Code and Section 2461, Title 28, United States Code.

  
\_\_\_\_\_  
Gregory K. Davis  
United States Attorney

A TRUE BILL:

s/signature redacted  
\_\_\_\_\_  
Foreperson of the Grand Jury

This indictment was returned in open court by the foreperson or deputy foreperson of the grand jury on this the 20<sup>th</sup> day of JANUARY, 2016.

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE